Network Working Group
Internet Draft
Intended status: Informational
Expires: August 2015

L. Dunbar
Huawei
M. Zarny
Goldman Sachs
C. Jacquenet
France Telecom
S. Chakrabarty
US Ignite

February 4, 2015

Interface to Network Security Functions Problem Statement
draft-dunbar-i2nsf-problem-statement-02.txt

Status of this Memo

Copyright Notice

Abstract

This draft describes the motivation, focused use cases, and the problem statement for Interface to Network Security Functions.

Table of Contents

1. Introduction

This draft describes the motivation, focused use cases, and the problem statement for Interface to Network Security Functions.

In the context of I2NSF, the term "Virtual Network Security Function" is used frequently to emphasize the point that the entities that consume the Network Security functions don't own or host them. Those network security functions can be achieved by physical appliances, or by VMs instantiated on servers.

1.1. Motivation

Enterprises are increasingly consuming network functions, especially the network security related functions that are not hosted at their promises. Some of the reasons driving up this demand are the desire (and the necessity) to:

- Implement stringent security functions at branch offices where minimal security infrastructures/capabilities exist;
- Provide interfaces for clients, and/or applications to dynamically alter security policies;
- Maintain consistent security policies across a large number of sites and devices.

According to [Gartner-2013], the demand for cloud-based security services is growing. Small and medium-sized businesses (SMBs) are increasingly adopting cloud-based security services to replace on-premises security tools, while larger enterprises are deploying a mix of traditional and cloud-based security services.

To efficiently meet the dynamic demand of security functions requests from clients, it is desirable to have mechanisms to:

- Specify concrete security rules (or attributes) for security functions hosted and managed by third party, and
- Have standardized mechanisms for clients, users, or applications to request/negotiate/validate security functions that are not physically located on the local premises.

Despite their increasing popularity, most common cloud security services do not yet have industry standards by which users/clients can request their desired services. (The "user-provider" relationship may exist between two different firms or between different domains of the same firm.)

1.2. Impact from Network Function Virtualization

The ETSI Network Function Virtualization (NFV) initiative brings out another management challenges for security policies to be enforced by distributed (virtual) network security functions (vNSF). Those trends require a standard interface to express, monitor, and manage the security policies on distributed security functions that may be running on different premises.

1.3. Network Security Functions under Consideration

There are many network functions being deployed and new ones are popping up with business and application demands. In order to have a concrete context for the protocols discussion, we start with the following network security related functions:

- Firewall
- Intrusion Detection System/ Intrusion Prevention System (IDS/IPS)

The reason for starting with security-related functions is due to the wide acceptance of security functions that are not running on customer/enterprise premises. Numerous security vendors are now leveraging cloud based models to deliver security solutions. This shift has occurred for a variety of reasons including greater economies of scale, streamlined delivery mechanisms, and the demand of business and applications for more sophisticated security functions that they do not have. Consumers, enterprise clients as well as applications are embracing the business model of requesting for security functions that do not run on their own premises on demand, also known as Network Security as a Service.

1.4. The scope of the proposed work

The Interface to vNSF (I2NSF) initiative is to identify how to express, monitor, and manage the security policies on distributed security functions that may be running on different premises. I2NSF also allows clients to communicate their specific security policies (request/monitor/report) to security functions.

There are two aspects of the I2NSF work:

- Service Layer, which is for clients to express, monitor, or manage their desired security policies for their designated traffic.

  This layer will leverage the existing protocols in RESTconf, AAA, SACM, and security policy expression using Role Based Access Control (RBAC), Mandatory Access Control (MAC), or Attribute based access control (ABAC).

- Functional layer, which is to specify the proper interface to the individual security functions or function instances when overall policies are enforced by a collection of security functions located in multiple premises.

The Interface to Network Security Functions (I2NSF) initiative aims at improving the dynamic allocation and operation of network security functions by documenting a global framework that would include protocol-based control and management interfaces, along with adequate data models. The information required for the provisioning, the configuration and the operation of network security functions will be exchanged through the said interfaces and protocols. The I2NSF initiative will also take into account the need for co-existing with legacy configuration and management systems used to allocate and operate network security functions, whether they are embedded in network devices or virtualized in data center environments, for example. The standard Interface to request/negotiate/allocate/operate (Virtual) Network Security Functions (I2NSF) is one of the necessary tools for operators and service providers to offer network security functions as a service to their corporate clients.

It is envisioned that clients of the I2NSF interfaces include Application Gateway, Security Administrator, service orchestration systems, even some security functions requests for more sophisticated functions when detect something suspicious.

Various aspects to I2NSF include:

- The mechanism for clients (applications) to request/negotiate/validate security policies that are enforced by security functions physically located in different premises, or administrative domain.

- Information/data model to configure and monitor the newly instantiate virtual security functions (NFV initiative).

The "requester <-> provider" relationship has different connotations in different scenarios:

- Client <-> Provider relationship, i.e. client requesting some network functions from its provider;
- Inter-domain, e.g. Domain A <-> Domain B relationship, i.e. one operator domain requesting some network functions from another operator domain, where "A" and "B" can be from same operator or different operators; or
- Application Gateways <-> Network relationship, i.e. an application gateway (e.g. cluster of servers) requesting some security policies for their designated traffic.

The security functions offered by third party need Bi-directional periodic communications among multiple entities for policies negotiation, validation, potentially re-directing traffic to higher level security functions, etc. Therefore, the service requires programmatic interfaces or protocol exchange, whereas API is conventionally associated with functional calls on one system.

The objective of the proposed work is to standardize the protocols (or the interface) and architecture for Requester and Provider to negotiate the functions needed as well as the associated attributes or security policies.

The proposed protocols between requester and provider can be used for the following scenarios:

- A Client requests a certain network security function from a provider
- The provider fulfills the request for example, by instantiating an instance of the service in question, or configures additional rules in an already provisioned vNSF.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

Cloud DC: The data centers that are not on premises of enterprises yet have the compute/storage resources that can be requested or purchased by the enterprises. What the enterprises actually get is Virtual Data Centers.

DC: Data Center

Domain: The term "Domain" in this draft has different connotations in different scenarios:

Client <-> Provider relationship, i.e. client requesting some network functions from its provider;

Domain A <-> Domain B relationship, i.e. one operator domain requesting some network functions from another operator domain; or

Applications <-> Network relationship, i.e. an application (e.g. cluster of servers) requesting some functions from network, etc.

Virtual Network Function: In the context of I2NSF, the term "Virtual Network Function" is used frequently to emphasize the point that the entities that consume the Network functions, mostly L4-L7 functions, don't own or host them. Those network functions can be achieved by physical appliances, or by VMs instantiated on common compute servers (i.e. the ETSI NFV defined Virtualized network functions).

Virtual Security Function: a security function that can be requested by one domain but may be owned or managed by another domain.

Cloud-based security functions: used interchangeably with the "Virtual Security Functions" in this draft.

3. Focused Use Cases

Many use cases have been described by [I2NSF-ACCESS], [I2NSF-DC] and the [I2NSF-Mobile]. To make I2NSF more focused, we will start with one use case that is described by all three use case drafts.

Enterprises, residential, and mobile customers are increasingly consuming network functions, especially the network security related functions that are not running on their premises. The ETSI Network Function Virtualization (NFV) initiative brings out another management challenges for security policies to be enforced by distributed (virtual) network security functions (vNSF). Those trends require a standard interface to express, monitor, and manage the security policies on distributed security functions that may be running on different premises.

One key aspect of those multiple premises hosted security functions is to have standard ways to express, monitor and verify security policies among distributed and virtual security functions.

The standard ways (I2NSF) to express security policies makes it possible for Application Gateway, e.g. Video Conference Controller, to dynamically inform the network security controller to have some specific encrypted flows by-passing some FW/IPS/IDS for a specific time span. Otherwise, some flows can't go through the FW/IPS/IDS because the payload is encrypted. Or require manually configuring a wide set of port ranges for calls to pass through (ex: ports 50,000 to 50,999) if there is a firewall placed in the middle of any enterprise deployment (very common for defense in depth postures). This causes a bigger attack surface area. I2NSF can dynamically create pinhole firewalls rules that are only active for when the call media session is alive. Once the session is over the pinhole policy is removed.

The standard interface (I2NSF) also makes it possible for Cloud DC to offer Virtual Firewall Function On Demand service.

Clients of cloud data center not only need virtual networks to interconnect their virtual compute/storage resources, but they also need virtual firewall services to enforce the proper communication policies. VPN clients, especially branch office access points, may need firewalls that are hosted by the VPN provider to be integrated with the VPN service.

Per [NW-2011], A cloud-based firewall is different from an on-premise one (aside from its location) in three key areas: scalability, availability and extensibility.

- Scalability: Cloud-based firewalls are designed to serve multiple customers and their increasing demand. Unlike with an on-premise firewall, upgrading a cloud-based firewall-e.g., for greater throughput-should be transparent to enterprise users.
- Availability: Cloud-based firewall providers tend to offer extremely high availability through their highly redundant and

resilient data centers. In contrast, most enterprises may not be able to offer "carrier-grade" high availability.

- Extensibility: Enterprises looking for vendor diversity can subscribe to cloud-based firewalls from different providers. Furthermore, additional features can be added more seamlessly, transparently.

4. Problem Space

Many vendors already offer Security as a Service in the cloud. However, all their solutions are proprietary, with different interfaces and different modes of operation.

There are no common interfaces/mechanisms for clients or applications to monitor or verify the required security policies or security functions. There is a lack of user-friendly service (policy) template.

I2NSF will only focus on the following problem spaces:

- Security Policy Layer, which is for clients to express, monitor, verify the needed security policies for their specific flows.

  Proper language has to be identified between clients and network security function controllers. This layer will leverage the existing protocols in RESTconf, AAA, SACM, and security policy expression using Role Based Access Control (RBAC), Mandatory Access Control (MAC), or Attribute-based access control (ABAC).

- Capability (or Functional) Layer, which specifies the information/data models to Security functions/devices (virtual & physical). This layer will leverage the existing protocols and data models defined by I2RS, Netconf, and NETMOD.

There are many other problems associated with Security Function on Demand that are out of the scope of I2NSF:

- Diverse security services:

  The I2NSF will only cover Firewall and IPS/IDS, may be extending to other security functions after re-chartering.

- Scalability:

  Not only diverse CPU/memory needed for different security functions can be difficult to manage, but the solution itself may have some limits, e.g. maximum number of firewall rules.

- Availability:

  The requested security functions or security policies might not be fulfilled. The negotiation protocol is not in the scope of I2NSF.

- Converting policies to vendor-specific configurations
- Dynamic features update

5. The Benefits

The goal of I2NSF is to specify standard mechanisms for clients to request security functions or security policies from another domain. The framework allows the clients to view, request, and/or verify the security functions/policies offered by different providers. This framework can make it easy for a cluster of devices requiring the similar security policies to have consistent policies across multiple sites.

The network service providers, with their physical access to a vast number of enterprises and consumers, are very well positioned to provide the "Security Function on Demand" services. The providers can act as security function brokers to their directly connected domains. They can offer a service catalog and standard mechanisms by which enterprises (or applications) can query request, or/and verify the needed security functions or policies.

With the standard interfaces for clients to request the needed security functions and policies, network operators can leverage their current VPN to enterprises and access to a vast population of end users to offer a set of consolidated Security solutions and policies. The IETF can play an instrumental role in defining this common interface and framework for network operators.

6. Related industry initiatives

6.1. Related IETF WGs

IETF NETCONF: I2NSF should consider using Netconf protocol for capability layer to communicate the security data models to the designated security functions.

NETMOD ACL Model: draft-ietf-netmod-acl-model-00 describes the very basic attributes for access control. I2NSF will extend the ACL data model to be more comprehensive, for example, extend to multiple actions and policies, and describes various services associated with the security functions under consideration.

For Firewall, I2NSF will specify the information model associated with various services of FW, such as stateful or deep packet inspection, packet/flow/stream filtering and redirect (remote and local), etc.

In addition, I2NSF has to specify the needed information model for the monitoring/reporting of FW.

I2RS: I2RS is thinking how to create interface between data and control plane, essentially be able to run an application like BGP somewhere else and then communicate the instruction to data plane how to act. I2NSF is looking specifically into expressing security policies in two layers. I2NSF should leverage the protocols developed by I2RS. I2NSF is only to develop the additional information models and data models for distributed security functions, like FW and IPS/IDS. The Policy structure specified by http://datatracker.ietf.org/doc/draft-hares-i2rs-bnp-info-model/ can be used by I2NSF to be extended to include recursive actions to other security functions.

IETF SFC is about mechanism of chaining together service functions while treating service functions as black box; VNFpool is about the reliability and availability of the virtualized network functions. But none of them address how service functions are requested, or how service functions are fulfilled.

Both SFC and VNFpool don't cover in-depth specification (e.g. rules for the requested FW) for clients to request its needed functions. In SFC & VNFpool, FW function is a black box, that is treated in same way as Video Optimization function. SFC/VNFpool don't cover the negotiation part, e.g. Client needs Rule x/y/z for FW, but the Provider can only offer x/z.

IETF SACM (Security Assessment and Continuous Monitoring) specifies the mechanisms to assess end point security. The end points can be routers, switches, clustered DB, installed piece of software. SACM is about "How to encode that policy in a manner where assessment can be automated". For examples:

- a Solaris 10 SPARC or Window 7 system used in a environment that requires adherence to a policy of Mission Critical Classified.
- rules like "The maximum password age must be 30 days" and "The minimum password age must be 1 day"

IETF midcom, nsis, pcp, (arguably) SOCKS have done some work that have some aspects related to or can be used by I2NSF.

6.2. Relationship with ETSI NFV

We believe that the I2NSF is one of the enabling tools for Network Security as a Service (NSaaS), which is a subset of VNF as a Service (VNFaaS) specified by ETSI NFV Group Specification Use Cases [gs_NFV]. The main benefits of virtualized network functions are increased flexibility to efficiently share the resources, and decreased setup and management costs. NFV defines the architecture to pool together many virtual network functions to be managed and consumed collectively.

NFV, with its heavy representation from service provider side, can define more detailed service model for VNFaaS and setting requirement for IETF's narrowly scoped I2NSF interface.

6.3. OpenStack Firewall/Security as a Service

Open source projects like OpenStack and CloudStack have begun to tackle the issues of interfaces to security functions but much work remains. There are many pieces of open sourced code, and there are a lot of areas not covered. The combined contributed source code is not comprehensive.

OpenStack completed the Firewall as a Service project and specified the set of APIs for Firewall services:
http://docs.openstack.org/admin-guide-cloud/content/fwaas_api_abstractions.html

OpenStack has defined the APIs for managing Security Groups:
http://docs.openstack.org/admin-guide-cloud/content/securitygroup_api_abstractions.html

The attributes defined by OpenStack Firewall/Security as a Service are very primitive. However they can be the basis of the information model for the I2NSF IETF initiative.

6.4. Security as a Service by Cloud Security Alliance

https://cloudsecurityalliance.org/research/secaas/#_get-involved

SaaS by CSA is at the initial stage of defining the scope of work.

6.5. Productive Eco-system with Open Source Communities

Our goal is to form a Collaborative Loop from IETF to Industry Open Source Communities (as Dave Ward said at IETF 91 Lunch session).

Open-source initiatives are not to be considered as an alternative to formal standardization processes. On the contrary, they are complementary, with the former acting as an enabler and accelerator of the latter. Open-source provides an ideal mechanism to quick prototyping and validating contending proposals, and demonstrating the feasibility of disruptive ideas that could otherwise not be considered. In this respect, open-source facilitates the engagement in the standardization process of small (and typically more dynamic) players such as start-ups and research groups, that would see better opportunities of being heard and a clearer rewards to their efforts. An open-source approach is extremely useful as well for the production of open reference implementations of the standards at the same (or even faster) pace they are defined. The availability of such reference implementations translate into much simpler interoperability and conformance assessments for both providers and users, and can become the basis for incremental differentiation of a common solution, thus allowing a cooperative competition ("coopetition") model.

7. Security Policies/functions negotiation

The protocol needed for this security function/policies negotiation may be somewhat correlated to the dynamic service parameter negotiation procedure [RFC7297]. The CPP template documented in RFC7297, even though currently covering only Connectivity, could be extended as a basis for the negotiation procedure. Likewise, the companion CPNP protocol could be a candidate to proceed with the negotiation procedure.

The "security as a service" would be a typical example of the kind of (CPP-based) negotiation procedures that could take place between a corporate customer and a service provider. However, more security specific parameters have to be considered by this proposed work.

8. Conclusion and Recommendation

The I2NSF aims at providing standard interfaces for clients to express, monitor, and manage their desired security policies, which can be instantiated on devices at different premises.

9. Manageability Considerations

TBD.

10. Security Considerations

TBD

11. IANA Considerations

This document requires no IANA actions. RFC Editor: Please remove this section before publication.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC7297] Boucadair, M., "IP Connectivity Provisioning Profile", RFC7297, April 2014.

12.2. Informative References

[I2NSF-ACCESS] A. Pastor, et al, "Access Use Cases for an Open OAM Interface to Virtualized Security Services", <draft-pastor-i2nsf-access-usecases-00>, Oct 2014.

[I2NSF-DC] M. Zarny, et al, "I2NSF Data Center Use Cases", <draft-zarny-i2nsf-data-center-use-cases-00>, Oct 2014.

[I2NSF-MOBILE] M. Qi, et al, "Integrated Security with Access Network Use Case", <draft-qi-i2nsf-access-network-usecase-00>, Oct 2014

[gs_NFV] ETSI NFV Group Specification, Network Functions Virtualizsation (NFV) Use Cases. ETSI GS NFV 001v1.1.1, 2013.

[Boucadair-framework] M. Boucadair, et al, "Differentiated Service Function Chaining Framework", < draft-boucadair-service-chaining-framework-00>; Aug 2013

[Gartner-2013] E. Messmer, "Gartner: Cloud-based security as a service set to take off", Network World, 31 October 2013

[NW-2011] J. Burke, "The Pros and Cons of a Cloud-Based Firewall", Network World, 11 November 2011

[SC-MobileNetwork] W. Haeffner, N. Leymann, "Network Based Services in Mobile Network", IETF87 Berlin, July 29, 2013

[Application-SDN] J. Giacomonni, "Application Layer SDN", Layer 123 ONF Presentation, Singapore, June 2013

13. Acknowledgments

Acknowledgements to Andy Malis for his review and contributions.

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Linda Dunbar
Huawei Technologies
5340 Legacy Drive, Suite 175
Plano, TX 75024, USA
Phone: (469) 277 5840
Email: ldunbar@huawei.com

Myo Zarny
Goldman Sachs
30 Hudson Street
Jersey City, NJ 07302
Email: myo.zarny@gs.com

Christian Jacquenet
France Telecom
Rennes 35000
France
Email: Christian.jacquenet@orange.com

Shaibal Chakrabarty
US Ignite
1776 Massachusetts Ave NW, Suite 601
Washington, DC 20036
Phone: (214) 708 6163
Email: shaibalc@us-ignite.org